

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-286989

(43)Date of publication of application : 13.10.2005

---

(51)Int.Cl.

H04L 12/28

H04L 12/56

---

(21)Application number : 2004-250816 (71)Applicant : NTT DOCOMO INC

(22)Date of filing : 30.08.2004 (72)Inventor : HAGIWARA JUNICHIRO  
AOKI HIDENORI  
UMEDA SEISHI

---

(30)Priority

Priority number : 2004058072 Priority date : 02.03.2004 Priority country : JP

---

### (54) COMMUNICATION TERMINAL AND AD HOC NETWORK ROUTE CONTROLLING METHOD

#### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a route controlling method etc. for preventing a risk of believing false route control information and for concealing address information etc. of a transmission reception terminal and a relay terminal as much as possible in an ad hoc network.

**SOLUTION:** A communication terminal capable of generating an ad hoc network route is configured by a transmitting/receiving unit for performing a communication with other communication terminals, a route request/generating unit for generating a route requesting message for requesting generation of an ad hoc network route, an address storing unit for storing an address of a self terminal and an address of a reception terminal, a random number generating unit for generating a random number, a certificate publishing unit for publishing a certificate of the self terminal, a digital signature producing unit for producing a digital signature of the self terminal, and a controlling unit for transmitting and receiving data configured from an address of the self terminal, an address of the reception terminal, a random number, a certificate, and a digital signature by adding to the route requesting message via the transmitting/receiving unit in response to an ad hoc network protocol.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]

It is a communication terminal which has a route request generating part which generates a route request message which requires generation of a transmission and reception section which generation of an ad hoc network course is possible and performs communication with other communication terminals and an ad hoc network course. :

An address storage section which memorizes an address of a self-terminal and an address of a receiving terminal;

A random number generation part which generates a random number;

A certificate issue section which publishes a certificate of a self-terminal;

A digital signature preparing part which creates a digital signature of a self-terminal;

A control section which transmits and receives data which added an address of a self-terminal, an address of a receiving terminal, the aforementioned random number, a certificate and a digital signature to said route request message and constituted them according to an ad hoc network protocol via said transmission and reception section;

A communication terminal \*\* constituted.

[Claim 2]

It is the communication terminal according to claim 1 and is a pan. :

A secret key treating part which creates a secret key and enciphers said at least some of data; it reaches.

Operation part which decodes received encrypted data;

A communication terminal \*\* constituted.

[Claim 3]

It is an ad hoc path control method for generating an ad hoc network among two or more communication terminals. :

A stage which carries out broadcast transmission of the data which added and constituted a transmit-terminal address, a receiving terminal address and a transmit-terminal digital signature to an ad hoc route request signal in a transmit terminal;

A stage which attests a transmit-terminal digital signature transmitted from a transmit terminal in a relay terminal and adds and carries out broadcast transfer of a relay terminal address and the relay terminal digital signature to said ad hoc route request signal;

A stage which attests said relay terminal digital signature and said transmit-terminal digital signature in a receiving terminal; it reaches.

A stage which addresses an ad hoc course reply signal which added and constituted a receiving terminal digital signature to said received data in said receiving terminal to said transmit terminal and transmits;

An ad hoc path control method \*\* constituted.

[Claim 4]

It is an ad hoc path control method for generating an ad hoc network among two or more communication terminals. :

A stage of data which added and constituted a transmit-terminal address and a receiving terminal address to an ad hoc route request signal in a transmit terminal which enciphers using a public key of a receiving terminal in part at least and carries out broadcast transmission of said data;

A stage which adds and carries out broadcast transfer of the relay terminal address to said ad hoc route request signal in a relay terminal;

A stage which addresses an ad hoc course reply signal which added said received data in a receiving terminal to said transmit terminal and transmits;

An ad hoc path control method \*\* constituted.

[Claim 5]

An ad hoc path control method which is the ad hoc path control method according to claim 3 and is characterized by having further a stage where said receiving terminal decrypts said received data in an attestation stage in the aforementioned receiving terminal using a self secret key.

[Claim 6]

An ad hoc path control method which is the ad hoc path control method according to claim 4 and is characterized by what said transmit terminal determines a session key and it has the stage of performing hybrid encryption using the session key for in an encryption stage in the aforementioned transmit terminal.

[Claim 7]

An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they are and is characterized by having further the stage of concealing the aforementioned relay terminal address.

[Claim 8]

An ad hoc path control method which is the ad hoc path control method according to claim 7 and is characterized by a stage of concealing the aforementioned relay terminal address comprising a stage of concealing information on an upstream relay terminal using a part of information on a relay terminal.

[Claim 9]

An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they are and is characterized by having further a stage which inserts a dummy address into said data.

[Claim 10]

An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they are and is characterized by having further a stage which inserts straw-man padding into said data.

[Claim 11]

An ad hoc network system which contains the communication terminal according to claim 1 or 2 as a transmit terminal and contains a relay terminal and a receiving terminal further.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

Especially this invention relates to the ad hoc network path control method which performs attestation and processing for privacy protection and the communication terminal for it about an ad hoc network path control method and the communication terminal for it.

[Background of the Invention]

[0002]

There is demand of connecting with a mobile radio communication network in connection with a huge expansion and the diversity of mobile communications demand from the mobile communication terminal in the exterior of the field which a mobile communications base station covers. From the direct one hop connection with a base station from the mobile communication terminal outside the cover region of a mobile communications base station being impossible. The method of using for a base station the wireless ad hoc network which makes multi-hop connection is proposed via other mobile communication terminals and simple relay stations installed temporarily. That is a wireless ad hoc network is a wireless network temporarily built by the personal digital assistant which a user uses the simple relay station installed temporarily etc. (refer to drawing 1). Each mobile communication terminal and a simple relay station build in an ad hoc routing protocol and spontaneous information is transmitted and received between each terminal according to this and they constitute an ad hoc network. Since information will be received by various terminals it is important to secure security and privacy in an ad hoc network.

[0003]

As an example of an ad hoc network when the routing demand from a terminal arises there is a DSR (Dynamic Source Routing) method which generates a course. In a DSR method a transmit terminal can send data using the course by getting to know the address of all the terminals (node) on the course to a receiving terminal. Since the terminal (node) which relays data can know the next destination using the channel information transmitted a relay terminal does not need to have channel information and it can be managed with comparatively light processing. By using an ad hoc network it becomes possible to provide cellular communications service an Internet access service etc. also to the mobile communication terminal out of the

communications area which a mobile radio communication network provides. In such a communication configuration it works as a component of an ad hoc network and the both sides of a mobile radio communication network and the communication terminal which bears mediation of the channel from an ad hoc network to a mobile radio communication network is called a gateway terminal (16 references of drawing 1). Here since the gateway terminal D is another name of the communication terminal which is carrying out direct continuation to the mobile radio communication network arbitrary communication terminals can turn into the gateway terminal D. When the gateway terminal D moves out of the area which a mobile radio communication network provides it does not get used to a gateway terminal any longer but becomes a mere mobile communication terminal.

[0004]

An ad hoc network is constituted as shown for example in drawing 1. Although the example of mobile radio communication explains an ad hoc network is not restricted to radio but is useful also in a wire communication. The moving terminal S (12) forms an ad hoc network according to an ad hoc path control protocol. It is connected to the gateway terminal D (16) via the relay terminal T1 (14) and the relay terminal T2 (15) and the mobile communication terminal S (12) constitutes the ad hoc network from an example of a graphic display. Since the gateway terminal D (16) is in the area which the base station B (18) covers it can connect with the base station B (18) via the gateway terminal D (16) and the moving terminal S (12) can receive the service from there (refer to patent documents 1).

[0005]

Here it is IETF (for the purpose of The Internet Engineering Task Force and the better architecture and the smooth operation of the Internet). Standardization of the Internet. The outline of the conventional example of the path control in DSR (Dynamic Source Routing) currently examined by MANET (Mobile Ad-hoc Networks) WG (task force) of the organization which is developing the volunteer activity at the center is shown in drawing 2 and drawing 3.

[0006]

The procedure of the conventional course establishment is explained referring to drawing 2 and drawing 3. Although the transmit terminal S (Source) shown in drawing 2 and drawing 3 is explained as a thing equivalent to the moving terminal S of drawing 1 it may not be restricted to this but a gateway terminal may be sufficient as it and they may be other moving terminals. Although the receiving terminal D (Destination) shown in drawing 2 and drawing 3 is explained as a thing equivalent to the gateway terminal D of drawing 1 it may not be restricted to this but may be a moving terminal. Although the relay terminal T (Transmitter) shown in drawing 2 and drawing 3 T1 and T2 are explained as a thing equivalent to the relay terminals 14 and 15 of drawing 1 they are not restricted to this. Since the relay terminal T1 of drawing 3 and T2 have composition and the the same function in drawing 2 the one relay terminal T represents

and is shown.

[0007]

When the transmit terminal S starts communication with the receiving terminal D, request/reply generating part 222 generates the signal of RREQ (Route REQuest) which is a control message for requiring generation of an ad hoc network route. The signal of RREQ is generated and the transmission and reception section 226 carries out broadcast transmission of the RREQ to a network. Address  $ADD_s$  of a transmit terminal and address  $ADD_d$  of a receiving terminal are read from the address storage section 227 and are added to RREQ and are transmitted together. An address may be an IP address for example. The information which restricts the hop number which carries out re transfer may also be included in control message PREQ.

[0008]

The relay terminal T1 which received control message RREQ by the transmission and reception section 246. If it turns out that its address  $ADD_{T1}$  memorized in the address storage section 247 is compared with address  $ADD_d$  which received and there is nothing at addressing to itself, its address  $ADD_{T1}$  will be added and RREQ will be transmitted by broadcasting.

[0009]

The transmission processing as the terminal T1 that the relay terminal T2 is also the same is performed.

[0010]

The receiving terminal D which received control message RREQ, adding what copied relay address information to a control message called RREP (Route REPLY) if their address and  $ADD_d$  which were memorized in the address storage section 267 are compared and it turns out that it is addressing to itself -- a unicast -- the transmit terminal S -- it sends a reply.

[0011]

The relay terminal T2 which received RREP will transmit this signal by a unicast if its address is discovered to a relay address list.

[0012]

The processing as the terminal T2 that the relay terminal T1 is also the same is performed.

[0013]

From the combination of address information  $ADD_s$  and  $ADD_d$ , the transmit terminal S which received RREP can recognize that this signal is the response to RREQ which he transmitted before and can know relay path information (S→T1→T2→D).

[Patent documents 1] JP2003-230167A

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0014]

However, in the DSR ad hoc network in conventional technology, since attestation of

RREQ which is a path control signal or RREP was omitted there was a danger of believing the mistaken path control information. Since transceiver person information the address information of a relay node etc. were stored in a header in the state where anyone can read a third party is able to specify a transceiver person and there were a problem of privacy etc.

[0015]

Then SUBJECT of this invention is providing the path control method etc. which can avoid the danger of believing the mistaken path control information by performing attestation of RREQ and RREP in an ad hoc network.

[0016]

It is providing the path control method etc. which can improve the privacy of the sender receiver terminal to a third party by concealing the address information of a sender receiver terminal or a relay terminal etc. as much as possible.

[Means for Solving the Problem]

[0017]

Generation of an ad hoc network course according to one feature of this invention for attaining above-mentioned SUBJECT is possible. A communication terminal which has a route request generating part which generates a route request message which requires generation of a transmission and reception section which performs communication with other communication terminals and an ad hoc network course A digital signature preparing part which creates a digital signature of a certificate issue section; self-terminal which publishes a certificate of a random number generation part; self-terminal which generates an address storage section; random number which memorizes an address of a self-terminal and an address of a receiving terminal; according to an ad hoc network protocol it comprises control-section; which transmits and receives data which added an address of a self-terminal and an address of a receiving terminal a random number a certificate and a digital signature to a route request message and constituted them via a transmission and reception section.

[0018]

Further such a mobile communication terminal may create a secret key and may have the operation part which decodes secret key treating part; and received encrypted data which encipher at least some data.

[0019]

An ad hoc path control method for generating an ad hoc network among two or more communication terminals according to one feature of this invention for attaining above-mentioned SUBJECT A stage which carries out broadcast transmission of the data which added and constituted a transmit-terminal address a receiving terminal address and a transmit-terminal digital signature to an ad hoc route request signal in a transmit terminal; In a relay terminal A stage which attests a transmit-terminal digital signature transmitted from a transmit terminal and adds and carries out broadcast transfer of a relay terminal address and the relay terminal digital signature to an ad

hoc route request signal; In a receiving terminal stage; and a receiving terminal which attest a relay terminal digital signature and a transmit-terminal digital signature it comprises stage; which addresses an ad hoc course reply signal which added and constituted a receiving terminal digital signature to received data to a transmit terminal and transmits.

[Effect of the Invention]

[0020]

If working example of this invention is followed the danger of believing the mistaken path control information is avoidable by performing attestation of RREQ and RREP. The privacy protection of the sender receiver terminal to a third party can be raised by concealing the address information of a sender receiver terminal or a relay terminal etc. as much as possible.

[Best Mode of Carrying Out the Invention]

[0021]

Hereafter each working example of this invention is described referring to Drawings. First the premise about each working example of this invention is expressed.

[0022]

- By a means of some kind all the nodes (terminal) hold the certificate of route CA (Certificate Authority certificate authority) can publish their own certificate and can create a secret key.

[0023]

- By a means of some kind the address and certificate of a communications partner can be known before a communication start.

[Work example 1]

[0024]

Working example 1 of this invention is described referring to drawing 4 and drawing 5. The moving terminal 400 according to working example of this invention it has request/reply generating part 422 the control section 424 the transmission and reception section 426 the address storage section 427 the address comparison part 428 the random number generation part 430 the certificate issue section 440 the digital signature preparing part 450 the secret key treating part 460 the operation part 470 and the verification part 480. This composition is not restricted to a transmit terminal but has composition also with same relay terminal and receiving terminal. This invention is not restricted to mobile radio communication but can be applied also to a wire communication.

[0025]

The transmission and reception section 426 carries out broadcast transmission of the route request control message RREQ generated in request/reply generating part 422 to a network.

[0026]

In working example 1 in RREQ attestation was applied between each hop



(namely between the transmit-terminal S → relay terminal T1 → relay terminal T2 → receiving terminals D) and attestation is applied only in between (namely between the receiving terminal D → transmit terminals S) by RREP as shown in drawing 5. It adds shading to a different portion from drawing 3 among drawing 5 and it is shown. Nonce shown in drawing 5 means the random number generated in the random number generation part 430. Cert<sub>x</sub> means the certificate of the terminal X which a certificate issue section publishes. Sig<sub>x</sub> is a digital signature by the terminal X. It is created by the digital signature preparing part.

[0027]

In DSR of a conventional example although attestation of RREQ and RREP is omitted these signals are attested in this example. Since every relay node is attested by RREQ it is thought by RREP of a reply that attestation of a between is enough.

[0028]

It explains per operation of each terminal below. The random number generation part 430 of the transmit terminal S determines the random number Nonce first. The certificate issue section 440 publishes Cert<sub>s</sub>. The control section 424 adds Nonce and own certificate Cert<sub>s</sub> to control message RREQ. The random number Nonce is added in order to protect a network from a resending attack. The receiving terminal adds a transmit terminal's own certificate to RREQ in order not to necessarily know the information on a transmit terminal. The digital signature preparing part 450 creates own digital signature Sig<sub>s</sub> Nonce and for all the fields of the signal RREQ which added certificate Cert<sub>s</sub>. The transmission and reception section 426 transmits to a network the signal RREQ with which Nonce, Cert<sub>s</sub> and Sig<sub>s</sub> were added by broadcasting.

[0029]

The verification part 480 of the relay terminal T1 which received the signal RREQ verifies Nonce contained in the received signal RREQ by a publicly known method. When Nonce is the same as the value of Nonce which received before it is recognized as this RREQ being retransmission of message and cancels. When Nonce is the first value to receive the verification part 480 verifies digital signature Sig<sub>s</sub> of a transmit terminal by a publicly known method using certificate Cert<sub>s</sub> added. If satisfactory as a result of verification it will check that ADD<sub>0</sub> is compared with its address and there is nothing at addressing to itself. Next address ADD<sub>T1</sub> and certificate Cert<sub>T1</sub> of relay terminal T1 self are added to the received signal and digital signature Sig<sub>T1</sub> of relay terminal T1 self is created to the whole added signal. ADD<sub>T1</sub>, Cert<sub>T1</sub> and RREQ that added Sig<sub>T1</sub> are transmitted to a network by broadcasting.

[0030]

The processing as the relay terminal T1 that the relay terminal T2 is also the same is performed. However digital signature Sig<sub>T1</sub> of the relay terminal T1 is verified using certificate Cert<sub>T1</sub> added. ADD<sub>T2</sub>, Cert<sub>T2</sub> and Sig<sub>T2</sub> are added to the RREQ signal received from the relay terminal T1 and it transmits to a network by broadcasting.

[0031]

The verification part 480 of the receiving terminal D which received the RREQ signal from the relay terminal T2 verifies Nonce. When Nonce is the same as the value of Nonce which received before it is recognized as this RREQ being retransmission of message and cancels. When Nonce is the first value to receive digital signature  $Sig_{T2}$  of a relay terminal is verified using certificate  $Cert_{T2}$  added.  $ADD_D$  is compared with its address and it recognizes that it is addressing to itself. Digital signature  $Sig_{T1}$  of a relay terminal is verified using certificate  $Cert_{T1}$  added. Digital signature  $Sig_S$  of a transmit terminal is verified using certificate  $Cert_S$  added. The turn of these processings may be changed.

[0032]

The copy of the contents of RREQ is added to the reply control message RREP generated by request/reply generating part of the receiving terminal D. Digital signature  $Sig_D$  of the receiving terminal D is created for all the fields of the RREP signal which added the copy of the contents of RREQ. RREP which added  $Sig_D$  is transmitted to transmit-terminal S by a unicast.

[0033]

The relay terminal T2 which received the RREP signal from the receiving terminal D verifies Nonce. Since its address  $ADD_{T2}$  can be discovered to a relay address list this signal is transmitted by a unicast as it is.

[0034]

The processing as the relay terminal T2 that the relay terminal T1 is also the same is performed.

[0035]

The verification part 480 of the transmit terminal S which received the RREP signal by the relay terminal T1 course performs the following processings after verifying Nonce first. Since its address  $ADD_S$  cannot be discovered to a relay address list it is verified whether it is RREP addressed to itself. He recognizes that it is the response to RREQ which transmitted before from the combination of  $ADD_S$ ,  $ADD_D$ , Nonce,  $Cert_S$  and  $Sig_S$ .  $Sig_D$  is verified. Sig for every relay path is verified. That is RREP is transposed to RREQ and  $Sig_D$  is removed. After verifying  $Sig_{T2}$ ,  $ADD_{T2}$ ,  $Cert_{T2}$  and  $Sig_{T2}$  are removed. After verifying  $Sig_{T1}$ ,  $ADD_{T1}$ ,  $Cert_{T1}$  and  $Sig_{T1}$  are removed. Relay path information (S->T1->T2->D) is become final and conclusive.

[Work example 2]

[0036]

Working example 2 of this invention is described referring to drawing 6 thru/or drawing 10. Although drawing 6 is the same figure as drawing 5 it shows the information about S and D which are exposed by the third party by shading. As shown in drawing 6 there is a problem that privacy cannot be protected in working example 1. For example in the area where a utilizing user is limited for round robin of a certificate if  $Cert_S$  pull there is a danger that the transmit terminal S will become clear.

[0037]

Thenworking example enciphered and concealed for the improvement in privacy protection so that only S and D may understand the shading field of drawing 6 is described. The common key encryption system which is a fundamental cipher system is a method which the receiving terminal D which the transmit terminal S enciphered plaintext data using the common keytransmitted the enciphered dataand received it decrypts using the same common key. From the place whose encryption and decryption are the same processings of an opposite directionit is also called a "symmetrical algorithm." High-speed processing is attained from using the same key as encryption and decryption. Howeverwhen a "common key" leaks to a third partythere is a disadvantageous point that the danger that all subsequent codes will be decoded becomes high.

[0038]

In the example shown in drawing 7a transient address is applied as address  $ADD_s$  of the transmit terminal S and the method which applied public-key-encryption-ization purely is explained to others. A public-key crypto system or an unsymmetrical algorithm is a method using the key which is differentrespectively as the key used for encryptionand a key used for decryption. Key of one of the two open to a partner is called a "public key." A receiving terminal creates a "secret key" and a "public key" in a pair. The direction of a "public key" is exhibited and the "secret key" is kept with the receiving terminal. A transmit terminal obtains the public key of a receiving terminalenciphers plaintext data using the keyand transmits encrypted data. The receiving terminal which received encrypted data decrypts encrypted data using the kept secret key.

[0039]

Here $E_x [y]$  means enciphering the plaintext y using the public key of X. In the transmit terminal S shown in drawing 7aaddress  $ADD_D$  of the receiving terminal DCertificate  $Cert_s$  and digital signature  $Sig_s$  of the transmit terminal S are enciphered by the public key of the receiving terminal D ( $E_D [ADD_D]E_D [Cert_s]E_D [Sig_s]$ ). The receiving terminal D which received these encrypted data is decrypted using the kept secret key. When sending a replydigital signature  $Sig_D$  of self is enciphered by the public key of the transmit terminal S ( $E_s [Sig_D]$ ). Howeverthere are the following problems in this method.

[0040]

1. Since the coding result to the same plaintextssuch as (original RSA)becomes the always same value depending on the algorithm of public key encryptionalthough  $ADD_D$  is unknowna "new" address called  $E_D [ADD_D]$  is always exposedand the danger of being pursued exists.

[0041]

2. The same danger exists also to a transient address.

[0042]

Therefore though the same value is enciphered the powerful measure [ direction / where a result different each time was obtained ] to disclosure of privacy is done more.

[0043]

Working example 2 which applied the hybrid code as shown in drawing 8 as working example over this problem is described. According to the hybrid cipher system the following processings are performed by a sender receiver terminal. Beforehand both the sender receiver terminal S and D have shared the common key. The receiving terminal D creates a "secret key" and a "public key" in a pair. The direction of a "public key" is exhibited and the "secret key" is kept with the receiving terminal D. The transmit terminal S obtains the public key of the receiving terminal D enciphers a common key using the public key and sends it to the receiving terminal D. Using the common key which the transmit terminal S enciphers symmetrical key encryption of plaintext data is performed and encrypted data is transmitted. The receiving terminal D which received the common key enciphered by the public key and encrypted data decrypts an encrypted common key using the kept secret key. Encrypted data is restored using the decrypted common key. In order for the plaintext data itself to perform encryption/decryption with a common cipher system with a quick speed high-speed processing speed is obtained. In order to improve confidentiality it is also possible to change the above-mentioned common key for every session. In that case the transmit terminal S performs symmetrical key encryption of data using a disposable common key (referred to as Session Key) for every session enciphers Session Key by a public key and notifies to the receiving terminal D.

[0044]

In working example shown in drawing 8a a transient address is applied to transmit-terminal address  $ADD_s$  and a hybrid code is applied to others. Below it explains focusing on different processing from drawing 3.

[0045]

The random number generation part 430 (refer to drawing 4) of the transmit terminal S determines transient address  $ADD_s$  of a transmit terminal at random. The random number generation part 430 determines the session key (Session Key) at random further and the secret key treating part 460 enciphers by the public key of the receiving terminal D and creates  $E_D$  [Session Key]. Since  $E_D$  [Session Key] can serve also as the meaning of Nonce it deletes Nonce in drawing 3 and transposes  $E_D$  [Session Key] to the position instead. The secret key treating part 460 obtains the output (pseudo-random number series) of a symmetrical key code using Session Key. The operation part 470 calculates the exclusive OR of transmit-terminal transient address  $ADD_s$ , receiving terminal address  $ADD_D$ , certificate  $Cert_s$  of a transmit terminal and digital signature  $Sig_s$  (signature for all the field) and the above-mentioned pseudo-random number series. The transmission and reception section 426 sets the whole to RREQ and carries out broadcast transmission.

[0046]

The relay terminal T1 which received RREQ assumes that RREQ which has specific length is RREQ from Sand does not perform verification of  $Sig_s$  (the management to this problem is mentioned later.)but carries out the same processing as drawing 3 and is transmitted. A relay terminal also carries out same processing and is transmitted.

[0047]

The receiving terminal D which received RREQ from the relay terminal T2 performs the following processings.

[0048]

Encrypted common key  $E_p$  [Session Key] which received is decrypted using its own secret key and a common key (Session Key) is obtained. The output (pseudo-random number series) of a symmetrical key code is obtained using Session Key obtained as a result of decoding. Data can be restored by taking the exclusive OR of the acquired pseudo-random number series and the field currently kept secret.

[0049]

In the case of a reply it re-enciphers using the newly created pseudo-random number series (it differs from the random number series at the time of reception) by the random number generation part of the receiving terminal D. That is the exclusive OR of a new pseudo-random number series and  $ADD_s$   $ADD_p$   $Cert_s$   $Sig_s$  and  $Sig_D$  is taken. Therefore the mask of the random number series of S and D will be given to  $ADD_s$  of  $RREP$   $ADD_p$   $Cert_s$  and  $Sig_s$  respectively.

[0050]

S which received RREP transmitted via the relay terminal T1 and T2 performs the following processings.

[0051]

When verifying whether it is RREP addressed to itself the pseudo-random number series which the receiving terminal D set up is removed. Although reference was not made in particular about the use mode of the symmetrical key code until now in order to output a pseudo-random number series use with CTR mode is common.

[0052]

The outline in CTR mode is shown in drawing 9. As for Initialization Vector (henceforth the following) it is desirable that it is sharable in secrecy among transceiver persons. As for a counter (henceforth the following) in order to synchronize among transceiver persons and to reduce the influence of a step-out it is desirable to add a raw value to a packet and to transmit it.

[0053]

Drawing 10 is the example which assumed CTR mode in the use mode of the symmetrical key code in drawing 8. It explains below focusing on different processing from drawing 5.

[0054]

IV decides to connect with Session Key and to transmit (it displays with the sign of

"||" below) and is taken as Seed=Session Key || Iv. It enables it to choose ct independently with the transmit terminal S and the receiving terminal D (it is respectively considered as  $ct_s$  and  $ct_D$ ) and it adds this field to the head of a packet. Since an order of a packet will leak to a third party if ct continues incrementally a sending person decides to assign a random value. Since ct also contained the implications of NonceED [Session Key] had been regarded as Nonce until now but below ct shall play the role of Nonce.

[Work example 3]

[0055]

Working example 3 of this invention is described referring to drawing 11 and 12. Although drawing 11 is the same figure as drawing 10 it shows the information about the relay terminal (node) exposed by the third party by shading. If the necessity for relay information is considered anew in order for the transmit terminal S and the receiving terminal D to perform Source Routing it is necessary to get to know the information on all the relay terminal but the relay terminal itself is enough if the following judgment can be performed.

[0056]

1. That check which is addressing to itself to RREQ justification of information from last relay terminal.

[0057]

2. Is he contained in a transmission address list to RREP or not?

[0058]

Therefore since disclosure of unnecessary information has the danger of becoming an offensive material it is desirable to conceal as much as possible also about the information on a relay terminal so that only the transmit terminal S and the receiving terminal D may be known. So below the example concealed so that only S and D may understand the shading field of drawing 11 for improvement in privacy is explained.

[0059]

In order to conceal the shading field of drawing 11 drawing 12 applies a public key temporarily and shows at RREQ the example to which the object of the symmetrical key code was expanded by RREP. It explains below focusing on different processing from drawing 8 and drawing 10.

[0060]

The random number generation part 430 of the transmit terminal S determines the pair of a secret key ( $K^-$ ) at random in transmission of RREQ a public key ( $K^+$ ) and temporarily temporarily. Although secret key  $K^-$  is added to RREQ public key  $K^+$  and temporarily temporarily and it transmits let only secret key  $K^-$  be an object of the exclusive OR of a pseudo-random number series temporarily.

[0061]

The relay terminal T2 which received RREQ carries out accumulation encryption of the information on a former relay terminal (in this case  $ADD_T, Cert_T, Sig_T$ ) using  $K^+$  from

itself. Even when the relay terminal which is malicious by carrying out accumulation encryption omits former relay terminal information by an inverse ramp from itself it can avoid that detection becomes impossible with the receiving terminal D.

[0062]

The receiving terminal D which received RREQ performs the following processings.

[0063]

Sig for every relay path is verified. After verifying  $Sig_{T2}ADD_{T2}Cert_{T2}$  and  $Sig_{T2}$  are removed. The whole information on a relay terminal is decoded temporarily using secret key K-.  $Sig_{T1}$  is verified.  $ADD_{T1}Cert_{T1}$  and  $Sig_{T1}$  are removed.  $Sig_s$  is verified.

[0064]

Generally only the number of times of relay guessed from the length of the whole relay terminal information will repeat processing of a following series. That is they are decoding verification of outermost Sig and processing of a series of removal of outermost additional information in secret key K- temporarily.

[0065]

When the receiving terminal D sends a reply to all the information copied from RREQ exclusive OR with the pseudo-random number series (it differs from the random number series at the time of reception) newly created with the receiving terminal D is taken it re-enciphers and RREP is created. The object domain of a mask pattern will be expanded and a mask pattern will be applied also to  $K-K+E_D$ .

[Seed]  $ADD_{T1}Cert_{T1}Sig_{T1}ADD_{T2}Cert_{T2}$  and  $Sig_{T2}$ .

[0066]

Since the mask pattern is hung on all the information copied from RREQ  $ADD_{T1}$  and  $ADD_{T2}$  are concealed and discernment of them becomes impossible in a relay terminal. Then it stores in the relay address list field in which the raw value of  $ADD_{T1}$  and  $ADD_{T2}$  was established newly.

[0067]

The transmit terminal S which received the RREP signal performs the following processings.

[0068]

Encrypted common key  $E_D$  [Seed] which received is decrypted and verified. Since its address  $ADD_s$  cannot be discovered to a relay address list a random number series is removed. He recognizes that it is the response to RREQ which transmitted before from the combination of  $ADD_sADD_DSeedCert_s$  and  $Sig_s$ .  $Sig_D$  is verified. Sig for every relay path is verified. That is RREP is transposed to RREQ and  $Sig_D$  is removed. After verifying  $Sig_{T2}ADD_{T2}Cert_{T2}$  and  $Sig_{T2}$  are removed. After verifying  $Sig_{T1}ADD_{T1}Cert_{T1}$  and  $Sig_{T1}$  are removed. Relay path information (S→T1→T2→D) is become final and conclusive.

[Work example 4]

[0069]

Working example 4 of this invention is described referring to drawing 13 and drawing

14. Although drawing 13 is the same figure as drawing 12 it shows the information about the relay terminal (node) exposed by the third party by shading. It is desirable to conceal as much as possible also about the address of a relay terminal so that the transmit terminal S the receiving terminal D and the relay terminal itself may be known. Then working example concealed so that the transmit terminal S the receiving terminal D and the relay terminal itself may understand the shading field of drawing 13 for improvement in privacy is described.

[0070]

Although there is the method of making  $ADD_{T1}$  and  $ADD_{T2}$  a transient address as easy management since the relay address same for a while will be applied through two or more packets the danger of being exposed of the relevance of a packet exists only by this method. Therefore structure stronger against disclosure of privacy is done by the direction where a different transient address for every packet is applied. In order to cope with this problem practical use of a public key and a hash function is considered temporarily.

[0071]

In order that drawing 14 may conceal the shading field of drawing 13 in RREQ it is the example which enciphered the random number by the public key temporarily and applied the hash function to the random number in RREP. It explains below focusing on different processing from drawing 9. The random number which  $rand_x$  determined at the terminal X and  $h(y)$  mean the hash value of y. A hash function means the existing function and procedure for summarizing from enumeration of character strings such as a document and a number to fixed length's data. The value outputted through a function is called a "hash value." The hash function "SHA-1" and "MD5" is typical and since all are one directional functions it is impossible to presume the original text from generated data. If both are compared in quest of the hash value of data at the both ends of a course when transmitting and receiving data through a communication line it can be investigated whether data is altered in the middle of communication.

[0072]

The relay terminal T1 which received RREQ sets up  $E_{K_r} [rand_{T1}]$  instead of address  $ADD_{T1}$  of self.

[0073]

T2 performs the same processing as T1.

[0074]

D which received RREQ acquires  $rand_{T1}$  and  $rand_{T2}$  and applies  $h(rand_{T1} || ct_b)$  and  $h(rand_{T2} || ct_b)$  instead of  $ADD_{T1}$  and the raw value of  $ADD_{T2}$ .

[0075]

T2 which received RREP recognizes its address as  $h(rand_{T2} || ct_b)$ .

[0076]

T1 performs the same processing as T2.



[0077]

The transmit terminal S which received RREP performs the following processings.

[0078]

$h(\text{rand}_S || \text{ct}_D)$  is inspected when discovering its address with a relay address list.  $\text{rand}_{T1}$  and  $\text{rand}_{T2}$  are acquired.

[Work example 5]

[0079]

Working example 5 of this invention is described referring to drawing 14 thru/or drawing 16.

[0080]

When drawing 14 is referred to the packet length of RREQ and the relay address list of RREP show that the danger that the information about the transmit terminal S and the receiving terminal D will leak as follows is high.

[0081]

- RREQ : packet length shows that the relay terminal T1 is next to the receiving terminal S.

[0082]

- RREP : if the relay terminal T1 and the relay terminal T2 conspire (conspiracy) a relay address list shows that the receiving terminal D is a next door (next door of ST1) of the relay terminal T2. Then the example which utilizes dummy information (random number) and conceals the information on the transmit terminal S and the receiving terminal D as much as possible to the transmit terminal S and the receiving terminal D by [ which is a relay terminal / that ] making it act like is explained.

[0083]

Drawing 15 gives each of the RREQ signal from the transmit terminal S and the RREP signal from the receiving terminal D dummy information and it is made to serve it as if both terminals were relay terminals. It explains below focusing on different processing from the above-mentioned example. The transmit terminal S gives dummy relay terminal information (Dummy1 Dummy2 which mean a part for 1 relay by drawing 15) into a RREQ signal. Since dummy information exists even if exposed of the information on the transmit terminal S it sees from a third party and distinction with a master station and a relay terminal does not stick.

[0084]

The relay terminal T1 which received the RREQ signal verifies  $\text{Sig}_S$ . Since verification of  $\text{Sig}_S$  was not completed in the example of the just before above it assumed that RREQ of specific length was RREQ from S and verification of  $\text{Sig}_S$  was not performed. In this example since S carried out \*\*\*\* of a relay terminal certificate  $\text{Cert}_S$  could be revealed and attestation became possible.

[0085]

D which received RREQ performs the following processings.

[0086]

It decrypts temporarily using secret key K—and Sig for every relay path is verified in an order from the re-outside and verification processing is repeated until Cert<sub>s</sub> appears. Although only the number of times of relay guessed from the length of the whole relay node information had repeated processing in the example of the just before above since S carries out \*\*\*\* of a relay terminal the method is inapplicable by this example.

[0087]

In the receiving terminal Da dummy address (drawing 15 DummyADD1 for two DummyADD2) is added to the relay address list of a RREP signal and exclusive OR with a pseudo-random number series is taken.

[0088]

The transmit terminal S which received the RREP signal verifies Sig for every relay path like the transmit terminal D.

[0089]

Here when drawing 15 is seen well it turns out that there is a danger that the information about the number of relay stages will leak from the packet length of a RREP signal. First of all the contents of the RREP signal are enough if the transmit terminal S and the receiving terminal D can be recognized and a third party does not need to identify. Then the example which conceals the history of a RREP signal as much as possible is explained below.

[0090]

Drawing 16 is the example which concealed the history of RREP as much as possible. It explains below focusing on different processing from the above-mentioned example.

[0091]

The receiving terminal D performs the following processings in creation of a RREP signal.

[0092]

Instead of RREP the transmit terminal S adds the 2nd identification field (RREP/Data) that can distinguish RREP or Data. Padding of dummy information (random number) is added (Dummy Padding in drawing 16). The Length field is added and the length except Dummy Padding is set up. The mask pattern which the receiving terminal D set up is covered over the 2nd identification field Dummy Padding and Length.

[0093]

The transmit terminal S which received RREP/Data performs the following processings after removing the mask pattern which the receiving terminal D set up.

[0094]

1. Recognize that it is RREP from the 2nd identification field.

[0095]

2. Remove Dummy Padding in consideration of the Length field.

[Work example 6]

[0096]

Working example 6 of this invention is shown in drawing 17. Working example 6 shown in drawing 17 is an example of the mode included all above-mentioned working example. Therefore explanation is omitted.

[Work example 7]

[0097]

Next temporarily supposing T2 is a malicious relay terminal the relay terminal T2 can cancel the information on the relay terminal T1 intentionally. Then the example for coping with such an evil deed is explained below.

[0098]

It explains with reference to drawing 17. The mechanism of detecting the information on the relay terminal T1 having been canceled by giving indivisible relation to the information on the relay terminal T1 and the information on terminal Dummy2 in front of that is considered.

[0099]

As shown in drawing 18 in the relay terminal T1 encryption by the block cipher which uses  $K_{T1} = h(\text{rand}_{T1}, \text{Cert}_{T1})$  based on the information on the relay terminal T1 as a key is given to the information on Dummy2 which is a terminal in front of that.  $\text{rand}_{T1}$  is a certificate of the terminal T1 in which a certificate issue section publishes the random number determined at the terminal T1 and  $\text{Cert}_{T1}$ .  
 $h(y)$  means the hash value of  $y$ .

[0100]

Also in the relay terminal T2 encryption by the block cipher which uses  $K_{T2} = h(\text{rand}_{T2}, \text{Cert}_{T2})$  based on the information on the relay terminal T2 as a key is given to the information on T1 which is a terminal in front of that. Therefore in order to restore this encryption the receiving terminal D needs to get to know right relay terminal information.

[0101]

Although this example was described taking the case of the case where Dummy is used the invention concerning this example can be applied also about the relay terminal which exists and can be applied also to the other various composition. The arbitrary terminal information of not only the last terminal information but the upper stream may be enciphered.

[0102]

Even if a malicious relay terminal cancels the information on an upstream relay terminal intentionally by having the above composition in the receiving terminal D the information on the terminal in front of the canceled relay terminal will be decoded correctly. In this way the receiving terminal D can detect this forged course.

[0103]

Thus according to this example without enlarging the processing load by a relay terminal so much forgery of the relay terminal information by a malicious relay terminal

can be prevented channel information can be concealed so that it cannot be forged and a transceiver person's privacy to a third party improves.

[Industrial applicability]

[0104]

In the radio or the wire communication field as which secrecy is required the communication terminal and ad hoc network path control method according to this invention can be used.

[Brief Description of the Drawings]

[0105]

[Drawing 1] It is a key map showing the outline of the conventional ad hoc network.

[Drawing 2] It is a schematic block diagram of the moving terminal in which the conventional ad hoc network construction is possible.

[Drawing 3] It is a chart which shows the data of the path control signal for the conventional ad hoc network construction.

[Drawing 4] It is a block diagram of the moving terminal according to working example of this invention.

[Drawing 5] It is a chart according to working example 1 which shows the data of the path control signal for ad hoc network construction.

[Drawing 6] It is a chart which shows the data of the path control signal for describing working example 2 and disclosure of the sender receiver terminal to a third party is shown.

[Drawing 7] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and the transient address is used for ADDS.

[Drawing 8] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and the hybrid code is used.

[Drawing 9] It is a key map according to working example 2 showing the outline in CTR mode.

[Drawing 10] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and CTR mode is used.

[Drawing 11] It is a chart which shows the data of the path control signal for describing working example 3 and disclosure of the relay information to a third party is shown.

[Drawing 12] It is a chart according to working example 3 which shows the data of the path control signal for ad hoc network construction and the public key is used temporarily.

[Drawing 13] It is a chart which shows the data of the path control signal for describing working example 4 and disclosure of the relay terminal address to a third party is shown.

[Drawing 14] It is a chart according to working example 4 which shows the data of the path control signal for ad hoc network construction and use of the hash function is

shown.

[Drawing 15] It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network construction and dummy information is added.

[Drawing 16] It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network construction and is the example which concealed the history of RREP as much as possible.

[Drawing 17] It is the chart which each working example contained altogether and which shows the data of the path control signal for ad hoc network construction.

[Drawing 18] It is a chart according to working example 7 which shows the data of the path control signal for ad hoc network construction and is an example which prevents cancellation of a relay terminal.

[Description of Notations]

[0106]

400 Moving terminal

422 Request/reply generating part

424 Control section

426 Transmission and reception section

427 Address storage section

428 Address comparison part

430 Random number generation part

440 Certificate issue section

450 Digital signature preparing part

460 Secret key treating part

470 Operation part

480 Verification part

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[0105]

[Drawing 1] It is a key map showing the outline of the conventional ad hoc network.

[Drawing 2] It is a schematic block diagram of the moving terminal in which the conventional ad hoc network construction is possible.

[Drawing 3] It is a chart which shows the data of the path control signal for the conventional ad hoc network construction.

[Drawing 4] It is a block diagram of the moving terminal according to working example of this invention.

[Drawing 5] It is a chart according to working example 1 which shows the data of the path control signal for ad hoc network construction.

[Drawing 6] It is a chart which shows the data of the path control signal for describing

working example 2 and disclosure of the sender receiver terminal to a third party is shown.

[Drawing 7] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and the transient address is used for ADDS.

[Drawing 8] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and the hybrid code is used.

[Drawing 9] It is a key map according to working example 2 showing the outline in CTR mode.

[Drawing 10] It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network construction and CTR mode is used.

[Drawing 11] It is a chart which shows the data of the path control signal for describing working example 3 and disclosure of the relay information to a third party is shown.

[Drawing 12] It is a chart according to working example 3 which shows the data of the path control signal for ad hoc network construction and the public key is used temporarily.

[Drawing 13] It is a chart which shows the data of the path control signal for describing working example 4 and disclosure of the relay terminal address to a third party is shown.

[Drawing 14] It is a chart according to working example 4 which shows the data of the path control signal for ad hoc network construction and use of the hash function is shown.

[Drawing 15] It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network construction and dummy information is added.

[Drawing 16] It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network construction and is the example which concealed the history of RREP as much as possible.

[Drawing 17] It is the chart which each working example contained altogether and which shows the data of the path control signal for ad hoc network construction.

[Drawing 18] It is a chart according to working example 7 which shows the data of the path control signal for ad hoc network construction and is an example which prevents cancellation of a relay terminal.

---

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-286989

(P2005-286989A)

(43) 公開日 平成17年10月13日(2005.10.13)

(51) Int. Cl. <sup>7</sup>		F I		テーマコード (参考)	
H04L	12/28	H04L	12/28	307	5K030
H04L	12/56	H04L	12/56	100D	5K033

審査請求 未請求 請求項の数 11 O L (全 20 頁)

(21) 出願番号	特願2004-250816 (P2004-250816)	(71) 出願人	392026693 株式会社エヌ・ティ・ティ・ドコモ
(22) 出願日	平成16年8月30日(2004.8.30)		東京都千代田区永田町二丁目1番1号
(31) 優先権主張番号	特願2004-58072 (P2004-58072)	(74) 代理人	100070150 弁理士 伊東 忠彦
(32) 優先日	平成16年3月2日(2004.3.2)		
(33) 優先権主張国	日本国 (JP)	(72) 発明者	萩原 淳一郎 東京都千代田区永田町二丁目1番1号 株式会社エヌ・ティ・ティ・ドコモ内
		(72) 発明者	青木 秀憲 東京都千代田区永田町二丁目1番1号 株式会社エヌ・ティ・ティ・ドコモ内
		(72) 発明者	梅田 成規 東京都千代田区永田町二丁目1番1号 株式会社エヌ・ティ・ティ・ドコモ内
		Fターム(参考)	5K030 GA15 JL01 LB05

最終頁に続く

(54) 【発明の名称】 通信端末及びアドホックネットワーク経路制御方法

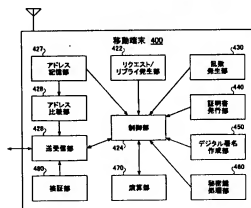
(57) 【要約】

【課題】 アドホックネットワークにおいて、誤った経路制御情報を信じてしまう危険性を回避し、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽する経路制御方法等を提供すること。

【解決手段】 アドホックネットワーク経路の生成が可能な通信端末が、他の通信端末との通信を行う送受信部；アドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部；自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；乱数を発生する乱数発生部；自己端末の証明書を発行する証明書発行部；自己端末のデジタル署名を作成するデジタル署名作成部；アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、乱数、証明書及びデジタル署名を経路要求メッセージに付加して構成したデータを、送受信部を介して送受信する制御部；から構成される。

【選択図】 図4

本発明の実施例に基いた移動端末のブロック図



## 【特許請求の範囲】

## 【請求項1】

アドホックネットワーク経路の生成が可能であり、他の通信端末との通信を行う送受信部とアドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部とを有する通信端末であって：

自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；

乱数を発生する乱数発生部；

自己端末の証明書を発行する証明書発行部；

自己端末のデジタル署名を作成するデジタル署名作成部；

アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、前記の乱数、証明書及びデジタル署名を前記経路要求メッセージに付加して構成したデータを、前記送受信部を介して送受信する制御部；

から構成される通信端末。

## 【請求項2】

請求項1記載の通信端末であってさらに：

秘密鍵を作成して、前記データの少なくとも一部を暗号化する秘密鍵処理部；及び

受信した被暗号化データを復号する演算部；

から構成される通信端末。

## 【請求項3】

複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法であって：

送信端末において、アドホック経路要求信号に送信端末アドレス、受信端末アドレス及び送信端末デジタル署名を付加して構成したデータをブロードキャスト送信する段階；

中継端末において、送信端末から送信された送信端末デジタル署名を認証し、前記アドホック経路要求信号に中継端末アドレス及び中継端末デジタル署名を付加してブロードキャスト転送する段階；

受信端末において、前記中継端末デジタル署名及び前記送信端末デジタル署名を認証する段階；及び

前記受信端末において、受信した前記データに受信端末デジタル署名を付加して構成したアドホック経路応答信号を前記送信端末に宛てて送信する段階；

から構成されるアドホック経路制御方法。

## 【請求項4】

複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法であって：

送信端末において、アドホック経路要求信号に送信端末アドレス及び受信端末アドレスを付加して構成したデータの少なくとも一部に受信端末の公開鍵を用いて暗号化を行い、前記データをブロードキャスト送信する段階；

中継端末において、前記アドホック経路要求信号に中継端末アドレスを付加してブロードキャスト転送する段階；

受信端末において、受信した前記データを付加したアドホック経路応答信号を前記送信端末に宛てて送信する段階；

から構成されるアドホック経路制御方法。

## 【請求項5】

請求項3に記載のアドホック経路制御方法であって、前記の受信端末における認証段階において、前記受信端末が、受信した前記データを自己の秘密鍵を用いて復号化する段階をさらに有することを特徴とするアドホック経路制御方法。

## 【請求項6】

請求項4に記載のアドホック経路制御方法であって、前記の送信端末における暗号化段階において、前記送信端末がセッションキーを決定し、そのセッションキーを用いたハイブリッド暗号化を行う段階を有する、ことを特徴とするアドホック経路制御方法。

10

20

30

40

50



## 【請求項 7】

上記請求項の何れかに記載のアドホック経路制御方法であって、前記の中継端末アドレスを隠蔽する段階をさらに有することを特徴とするアドホック経路制御方法。

## 【請求項 8】

請求項 7 に記載のアドホック経路制御方法であって、前記の中継端末アドレスを隠蔽する段階が、中継端末の情報の一部を利用して上流の中継端末の情報を隠蔽する段階から成ることを特徴とするアドホック経路制御方法。

## 【請求項 9】

上記請求項の何れかに記載のアドホック経路制御方法であって、前記データ中にダミーアドレスを挿入する段階をさらに有することを特徴とするアドホック経路制御方法。

## 【請求項 10】

上記請求項の何れかに記載のアドホック経路制御方法であって、前記データ中にダミーパディングを挿入する段階をさらに有することを特徴とするアドホック経路制御方法。

## 【請求項 11】

請求項 1 又は 2 に記載の通信端末を送信端末として含み、さらに、中継端末及び受信端末を含むアドホックネットワークシステム。

## 【発明の詳細な説明】

## 【技術分野】

## 【0001】

本発明は、アドホックネットワーク経路制御方法及びそのための通信端末に関し、特に認証やプライバシー保護のための処理を行うアドホックネットワーク経路制御方法及びそのための通信端末に関する。

## 【背景技術】

## 【0002】

移動通信需要の急拡大・多様性に伴い、移動通信基地局がカバーする領域の外部にある移動通信端末から移動通信網へ接続することの必要がある。移動通信基地局のカバー領域外にある移動通信端末から基地局への直接的なワンホップ接続が不可能であることから、他の移動通信端末や一時的に設置した簡易中継局を介して基地局にマルチホップ接続するワイヤレスアドホックネットワークを利用する方法が提案されている。すなわち、ワイヤレスアドホックネットワークとは、ユーザの利用する携帯端末や一時的に設置した簡易中継局等によって一時的に構築される無線ネットワークである（図 1 参照）。各移動通信端末および簡易中継局は、アドホックルーティングプロトコルを内蔵し、これに従って各端末間で自発的な情報の送受信を行い、アドホックネットワークを構成する。アドホックネットワークでは、種々の端末に情報が受信されてしまうことから、セキュリティ、プライバシーを確保することが重要である。

## 【0003】

アドホックネットワークの一例として、端末からの経路設定要求が生じた際に経路を生成する DSR (Dynamic Source Routing) 方式がある。DSR 方式では、送信端末が、受信端末までの経路上の全端末（ノード）のアドレスを知ることにより、その経路を使ってデータを送ることができる。データの中継する端末（ノード）は、転送される経路情報を利用して次の転送先を知ることができるため、中継端末が経路情報を持つ必要がなく、比較的軽い処理で済む。アドホックネットワークを利用することにより、移動通信網の提供する通信エリアの外にある移動通信端末に対しても、セルラー通信サービスやインターネット接続サービス等を提供することが可能となる。このような通信形態において、アドホックネットワークと移動通信網の双方の構成要素として稼働し、アドホックネットワークから移動通信網への通信路の橋渡しを担う通信端末を、関門端末と呼ぶ（図 1 の 16 参照）。ここで、関門端末 D は、移動通信網に直接接続している通信端末の別称であるから、任意の通信端末が関門端末 D となることができる。また、関門端末 D が移動通信網の提供するエリアの外へと移動した場合、もはや関門端末にはなれず、単なる移動通信端末となる。

## 【0004】

10

20

30

40

50

アドホックネットワークは、例えば図1に示すように構成される。移動無線通信の例で説明するが、アドホックネットワークは、無線に限られず有線通信においても有用である。移動端末S(12)は、アドホック経路制御プロトコルに従って、アドホックネットワークを形成する。図示の例では、移動通信端末S(12)が中継端末T1(14)及び中継端末T2(15)を経由して関門端末D(16)に接続されて、アドホックネットワークを構成している。関門端末D(16)が基地局B(18)のカバレッジするエリア内にいるので、移動端末S(12)は関門端末D(16)を経由して基地局B(18)に接続してそこからのサービスを受けることができる(特許文献1参照)。

【0005】

ここで、IETF(The Internet Engineering Task Force, インターネットのよりよいアーキテクチャやスムーズなオペレーションを目的に、インターネットの標準化を中心にボランティア活動を展開している団体)のMANET(Mobile Ad-hoc Networks) WG(作業部会)で検討されているDSR(Dynamic Source Routing)における経路制御の従来例の概要を図2及び図3に示す。

【0006】

図2及び図3を参照しながら、従来の経路確立の手順を説明する。図2及び図3に示す送信端末S(Source)は、図1の移動端末Sに相当するものとして説明するが、これに限られず、関門端末でも良いし、他の移動端末であっても良い。図2及び図3に示す受信端末D(Destination)は、図1の関門端末Dに相当するものとして説明するが、これに限られず、移動端末であっても良い。図2及び図3に示す中継端末T(Transmitter)、T1、T2は、図1の中継端末14、15に相当するものとして説明するが、これに限らない。図3の中継端末T1、T2は構成及び機能が同じであるので、図2においては1つの中継端末Tが代表して示されている。

【0007】

送信端末Sが受信端末Dとの通信を開始する際、リクエスト/リプライ発生部222が、アドホックネットワーク経路の生成を要求するための制御メッセージであるRREQ(Route Request)という信号を発生させ、送受信部226がRREQをネットワークヘブロードキャスト送信する。送信端末のアドレスADD<sub>S</sub>と受信端末のアドレスADD<sub>D</sub>がアドレス記憶部227から読み出され、RREQに付加され、一緒に送信される。アドレスは、例えばIPアドレスであってよい。制御メッセージPREQには、再転送するホップ数を制限する情報を含んでも良い。

【0008】

制御メッセージRREQを送受信部246によって受信した中継端末T1は、アドレス記憶部247内に記憶された自分のアドレスADD<sub>T1</sub>と受信したアドレスADD<sub>D</sub>とを比較して、自分宛で無いことが分かると、自分のアドレスADD<sub>T1</sub>を付加して、RREQをブロードキャストで転送する。

【0009】

中継端末T2も端末T1と同様の転送処理を行う。

【0010】

制御メッセージRREQを受信した受信端末Dは、アドレス記憶部267内に記憶された自分のアドレスとADD<sub>D</sub>を比較して自分宛であることが分かると、RREP(Route Reply)という制御メッセージに中継アドレス情報をコピーしたものを付加して、ユニキャストで送信端末Sへと返信する。

【0011】

RREPを受信した中継端末T2は、中継アドレスリストに自分のアドレスを発見すると、この信号をユニキャストで転送する。

【0012】

中継端末T1も端末T2と同様の処理を行う。

【0013】

RREPを受信した送信端末Sは、アドレス情報ADD<sub>S</sub>とADD<sub>D</sub>の組み合わせから、この信号は

10

20

30

40

50

自分が以前に送信したRREQに対する応答であることを認識でき、中継経路情報(S→T1→T2→D)を知ることができる。

【特許文献1】特開2003-230167号公報

【発明の開示】

【発明が解決しようとする課題】

【0014】

しかしながら、従来技術におけるDSRアドホックネットワークでは、経路制御信号であるRREQやRREPの認証を行っていないため、誤った経路制御情報を信じてしまう危険性があった。また、送受信者情報や中継ノードのアドレス情報等を誰でも読める状態でヘッダに格納するため、第三者が送受信者を特定する事が可能であり、プライバシー上の問題等があった。

【0015】

そこで、本発明の課題は、アドホックネットワークにおいてRREQとRREPの認証を行うことにより、誤った経路制御情報を信じてしまう危険性を回避できるような経路制御方法を提供することである。

【0016】

また、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽することにより、第三者に対する送受信端末のプライバシーを向上できるような経路制御方法等を提供することである。

【課題を解決するための手段】

【0017】

上記の課題を達成するための本発明の一特徴に従った、アドホックネットワーク経路の生成が可能であり、他の通信端末との通信を行う送受信部とアドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部とを有する通信端末は、自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；乱数を発生する乱数発生部；自己端末の証明書を発行する証明書発行部；自己端末のデジタル署名を作成するデジタル署名作成部；アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、乱数、証明書及びデジタル署名を経路要求メッセージに付加して構成したデータを、送受信部を介して送受信する制御部；から構成される。

【0018】

このような移動通信端末はさらに、秘密鍵を作成して、データの少なくとも一部を暗号化する秘密鍵処理部；及び受信した被暗号化データを復号する演算部を有しても良い。

【0019】

上記の課題を達成するための本発明の一特徴に従った、複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法は、送信端末において、アドホック経路要求信号に送信端末アドレス、受信端末アドレス及び送信端末デジタル署名を付加して構成したデータをブロードキャスト送信する段階；中継端末において、送信端末から送信された送信端末デジタル署名を認証し、アドホック経路要求信号に中継端末アドレス及び中継端末デジタル署名を付加してブロードキャスト転送する段階；受信端末において、受信したデータに受信端末デジタル署名を付加して構成したアドホック経路応答信号を送信端末に宛てて送信する段階；から構成される。

【発明の効果】

【0020】

本発明の実施例に従えば、RREQとRREPの認証を行うことで、誤った経路制御情報を信じてしまう危険性を回避することができる。また、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽することにより、第三者に対する送受信端末のプライバシー保護を向上させることができる。

【発明を実施するための最良の形態】

【0021】

10

20

30

40

50

以下、図面を参照しながら本発明の各実施例について説明する。先ず、本発明の各実施例についての前提を述べる。

#### 【0022】

・何らかの手段によって、全ノード（端末）がルートCA（Certificate Authority、認証局）の証明書を保持しており、自分の証明書を発行でき、秘密鍵を作成可能である。

#### 【0023】

・何らかの手段によって、通信開始前に通信相手のアドレスと証明書を知ることができる。

#### 【実施例1】

#### 【0024】

図4及び図5を参照しながら、本発明の実施例1を説明する。本発明の実施例に従った移動端末400は、リクエスト／リプライ発生部422、制御部424、送受信部426、アドレス記憶部427、アドレス比較部428、乱数発生部430、証明書発行部440、デジタル署名作成部450、秘密鍵処理部460、演算部470及び検証部480を有している。この構成は、送信端末に限られず、中継端末や受信端末も同様な構成を有する。本発明は、移動無線通信に限られず、有線通信に対しても適用可能である。

#### 【0025】

リクエスト／リプライ発生部422で発生された経路要求制御メッセージRREQを、送受信部426がネットワークへブロードキャスト送信する。

#### 【0026】

実施例1においては、図5に示されているように、RREQでは、各ホップ間（すなわち、送信端末S→中継端末T1→中継端末T2→受信端末Dの間）に認証を適用し、RREPでは、エンド間（すなわち、受信端末D→送信端末Sの間）のみに認証を適用している。図5のうち図3と異なる部分は、網掛けして示している。図5に示すNonceは、乱数発生部430にて発生された乱数を意味する。Cert<sub>x</sub>は、証明書発行部が発行する端末Xの証明書を意味する。Sig<sub>x</sub>は、端末Xによるデジタル署名であり、デジタル署名作成部により作成される。

#### 【0027】

従来例のDSRにおいては、RREQ、RREPの認証を行っていないが、本実施例においては、これらの信号の認証を行うものである。RREQで中継ノード毎の認証を行うので、返信のRREPではエンド間の認証で十分であると考えられる。

#### 【0028】

以下に各端末の動作につき説明する。先ず送信端末Sの乱数発生部430が、乱数Nonceを決定する。証明書発行部440が、Cert<sub>s</sub>を発行する。制御部424が、制御メッセージRREQにNonceと自身の証明書Cert<sub>s</sub>を付加する。乱数Nonceを付加するのは、ネットワークを再送攻撃から守るためである。また、受信端末は送信端末の情報を必ずしも知るわけではないため、RREQに送信端末自身の証明書を付加しておく。Nonceと証明書Cert<sub>s</sub>を付加した信号RREQの全フィールドを対象として、デジタル署名作成部450が、自身のデジタル署名Sig<sub>s</sub>を作成する。Nonce、Cert<sub>s</sub>及びSig<sub>s</sub>が付加された信号RREQを、送受信部426がブロードキャストでネットワークに送信する。

#### 【0029】

信号RREQを受信した中継端末T1の検証部480が、公知の方法で、受信した信号RREQに含まれるNonceの検証を行う。もし、Nonceが、以前受信したNonceの値と同じ場合には、今回のRREQが再送信であると認識して破棄する。Nonceが初めて受信する値である場合には、検証部480が、付加されている証明書Cert<sub>s</sub>を用いて、送信端末のデジタル署名Sig<sub>s</sub>を公知の方法で検証する。検証の結果、問題が無ければ、ADD<sub>0</sub>と自分のアドレスとを比較して自分宛で無いことを確認する。次に、受信した信号に中継端末T1自身のアドレスADD<sub>T1</sub>と証明書Cert<sub>T1</sub>とを付加し、付加した信号全体に対して中継端末T1自身のデジタル署名Sig<sub>T1</sub>を作成する。ADD<sub>T1</sub>、Cert<sub>T1</sub>、Sig<sub>T1</sub>を付加したRREQをネットワークへブロードキャストで転送する。

10

20

30

40

50

## 【0030】

中継端末T2も中継端末T1と同様の処理を行う。ただし、付加されている証明書Cert<sub>T1</sub>を用いて、中継端末T1のデジタル署名Sig<sub>T1</sub>を検証し、中継端末T1から受信したRREQ信号にADD<sub>T2</sub>、Cert<sub>T2</sub>、Sig<sub>T2</sub>を付加してネットワークへブロードキャストで転送する。

## 【0031】

中継端末T2からのRREQ信号を受信した受信端末Dの検証部480は、Nonceの検証を行う。もし、Nonceが、以前受信したNonceの値と同じ場合には、今回のRREQが再送信であると認識して破棄する。Nonceが初めて受信する値である場合には、付加されている証明書Cert<sub>T2</sub>を用いて、中継端末のデジタル署名Sig<sub>T2</sub>を検証する。ADD<sub>D</sub>と自分のアドレスとを比較して自分宛であることを認識する。付加されている証明書Cert<sub>T1</sub>を用いて、中継端末のデジタル署名Sig<sub>T1</sub>を検証する。付加されている証明書Cert<sub>S</sub>を用いて、送信端末のデジタル署名Sig<sub>S</sub>を検証する。これらの処理の順番は、変更しても良い。

10

## 【0032】

受信端末Dのリクエスト／リプライ発生部により発生した応答制御メッセージRREPに対して、RREQの内容のコピーを付加する。RREQの内容のコピーを付加したRREP信号の全フィールドを対象として、受信端末Dのデジタル署名Sig<sub>D</sub>を作成する。Sig<sub>D</sub>を付加したRREPをユニキャストで送信端末S宛に送信する。

## 【0033】

受信端末DからのRREP信号を受信した中継端末T2は、Nonceの検証を行う。中継アドレスリストに自分のアドレスADD<sub>T2</sub>を発見できるため、この信号をそのままユニキャストで転送する。

20

## 【0034】

中継端末T1も中継端末T2と同様の処理を行う。

## 【0035】

中継端末T1経由でRREP信号を受信した送信端末Sの検証部480は、先ずNonceの検証を行った後、以下の処理を行う。中継アドレスリストに自分のアドレスADD<sub>S</sub>を発見できないため、自分宛のRREPであるかどうかを検証する。ADD<sub>S</sub>、ADD<sub>D</sub>、Nonce、Cert<sub>S</sub>、Sig<sub>S</sub>の組み合わせから、自分が以前に送信したRREQに対する応答であることを認識する。Sig<sub>D</sub>を検証する。中継経路毎のSigを検証する。すなわち、RREPをRREQに置きかえてSig<sub>D</sub>を除去する。Sig<sub>T2</sub>を検証した後、ADD<sub>T2</sub>、Cert<sub>T2</sub>、Sig<sub>T2</sub>を除去する。Sig<sub>T1</sub>を検証した後、ADD<sub>T1</sub>、Cert<sub>T1</sub>、Sig<sub>T1</sub>を除去する。中継経路情報(S→T1→T2→D)を確定する。

30

## 【実施例2】

## 【0036】

図6乃至図10を参照しながら、本発明の実施例2について説明する。図6は、図5と同様な図であるが、第三者に露呈されるSとDに関する情報を網掛けで示している。図6に示されるように、実施例1においては、プライバシーを保護できないという問題点がある。例えば、利用ユーザが限定される地域では、証明書の総当たりで、Cert<sub>S</sub>が、ひいては送信端末Sが判明してしまう危険性がある。

## 【0037】

そこで、プライバシー保護向上のために、図6の網掛けフィールドをSとDにしか分からないように暗号化して隠蔽する実施例を説明する。基本的な暗号方式である共通鍵暗号方式は、送信端末Sが平文データを共通鍵を用いて暗号化し、暗号化したデータを送信し、それを受信した受信端末Dが同じ共通鍵を用いて復号化する方式である。暗号化と復号化が逆方向の同じ処理であるところから、「対称アルゴリズム」とも呼ばれる。暗号化と復号化に同じ鍵を使うことから、高速な処理が可能となる。しかし、第三者に「共通鍵」が漏れてしまうと、その後の暗号を全て解説されてしまう危険性が高くなるという不利点がある。

40

## 【0038】

図7に示す例では、送信端末SのアドレスADD<sub>S</sub>として一時アドレスを適用し、その他には公開鍵暗号化を純粹に適用した方法を説明する。公開鍵暗号方式又は非対称アルゴリズム

50

ムとは、暗号化に使用する鍵と復号化に使用する鍵として、それぞれ違う鍵を用いる方式である。相手に公開した片方の鍵を「公開鍵」と呼ぶ。受信端末が「秘密鍵」と「公開鍵」をペアで作成する。「公開鍵」の方は公開し、「秘密鍵」は受信端末で保管しておく。送信端末は、受信端末の公開鍵を入手し、その鍵を用いて平文データの暗号化を行い、被暗号化データを送信する。被暗号化データを受信した受信端末は、保管しておいた秘密鍵を用いて被暗号化データを復号化する。

#### 【0039】

ここで、 $E_x[y]$  とは  $X$  の公開鍵を用いて平文  $y$  を暗号化することを意味している。図 7 に示す送信端末  $S$  において、受信端末  $D$  のアドレス  $ADD_D$ 、送信端末  $S$  の証明書  $Cert_S$  及びデジタル署名  $Sig_S$  を、受信端末  $D$  の公開鍵で暗号化 ( $E_D[ADD_D]$ ,  $E_D[Cert_S]$ ,  $E_D[Sig_S]$ ) する。これらの被暗号化データを受信した受信端末  $D$  は、保管しておいた秘密鍵を用いて復号化する。返信する際には、自己のデジタル署名  $Sig_D$  を、送信端末  $S$  の公開鍵で暗号化 ( $E_S[Sig_D]$ ) する。しかし、この方法には以下の問題がある。

#### 【0040】

1. 公開鍵暗号のアルゴリズムによっては (オリジナルの RSA 等)、同じ平文に対する暗号結果は常に同じ値になるため、 $ADD_D$  は不明だが  $E_D[ADD_D]$  という “新しい” アドレスが常に露呈され、追跡される危険性が存在する。

#### 【0041】

2. 一時アドレスに対しても、同じような危険性が存在する。

#### 【0042】

従って、同じ値を暗号化としても、毎回異なる結果が得られるようにした方が、よりプライバシーの漏洩に対する強い対策ができる。

#### 【0043】

この問題に対する実施例として、図 8 に示すようなハイブリッド暗号を適用した実施例 2 を説明する。ハイブリッド暗号方式によれば、送受信端末で以下のような処理を行う。予め、送受信端末  $S$ 、 $D$  双方が共通鍵を共有している。受信端末  $D$  が「秘密鍵」と「公開鍵」をペアで作成する。「公開鍵」の方は公開し、「秘密鍵」は受信端末  $D$  で保管しておく。送信端末  $S$  は、受信端末  $D$  の公開鍵を入手し、その公開鍵を用いて共通鍵を暗号化して受信端末  $D$  に送る。送信端末  $S$  が、暗号化した共通鍵を用いて、平文データの対称鍵暗号化を行い、被暗号化データを送信する。公開鍵で暗号化された共通鍵と被暗号化データを受信した受信端末  $D$  は、保管しておいた秘密鍵を用いて被暗号化共通鍵を復号化する。その復号化された共通鍵を用いて、被暗号化データを復元する。平文データ自体は、速度の速い共通暗号化方式で暗号化/復号化を行うため、高速の処理速度が得られる。秘密性を高めるために、上記の共通鍵をセッション毎に変更することも可能である。その場合には、送信端末  $S$  が、セッション毎に使い捨ての共通鍵 (Session Key と呼ぶ) を用いてデータの対称鍵暗号化を行い、Session Key を公開鍵で暗号化して受信端末  $D$  に通知する。

#### 【0044】

図 8 に示す実施例においては、送信端末アドレス  $ADD_S$  には一時アドレスを適用し、その他にはハイブリッド暗号を適用する。以下に、図 3 とは異なる処理を中心に説明する。

#### 【0045】

送信端末  $S$  の乱数発生部 430 (図 4 参照) が、送信端末の一時アドレス  $ADD_S$  をランダムに決定する。乱数発生部 430 がさらにセッションキー (Session Key) をランダムに決定し、秘密鍵処理部 460 が受信端末  $D$  の公開鍵で暗号化して、 $E_D[Session Key]$  を作成する。 $E_D[Session Key]$  は Nonce の意味も兼ねることができるため、図 3 における Nonce を削除し、代わりに  $E_D[Session Key]$  をその位置に置きかえる。秘密鍵処理部 460 が、Session Key を用いて対称鍵暗号の出力 (疑似乱数系列) を得る。演算部 470 が、送信端末一時アドレス  $ADD_S$ 、受信端末アドレス  $ADD_D$ 、送信端末の証明書  $Cert_S$  及びデジタル署名  $Sig_S$  (全てのフィールドを対象とした署名) と上記疑似乱数系列との排他的論理和を計算する。送受信部 426 が、全体を RREQ としてブロードキャスト送信する。

10

20

30

40

50

【0046】

RREQを受信した中継端末T1は、特定の長さを有するRREQはSからのRREQであると想定してSig<sub>S</sub>の検証は行わず（この問題に対する対処は、後述する。）、図3と同様な処理をして転送する。中継端末も同様な処理をして、転送する。

【0047】

中継端末T2からRREQを受信した受信端末Dは以下の処理を行う。

【0048】

受信した被暗号化共通鍵E<sub>0</sub> [Session Key] を自分の秘密鍵を用いて復号化して、共通鍵 (Session Key) を得る。復号の結果得られたSession Keyを用いて、対称鍵暗号の出力 (疑似乱数系列) を得る。得られた疑似乱数系列と秘匿されているフィールドとの排他的論理和を取ることによって、データを復元することができる。

10

【0049】

返信の際には、受信端末Dの乱数発生部で新たに作成した疑似乱数系列（受信時の乱数系列とは異なる）を用いて再暗号化する。すなわち、新しい疑似乱数系列とADD<sub>S</sub>, ADD<sub>D</sub>, Cert<sub>S</sub>, Sig<sub>S</sub>, SigDとの排他的論理和を取る。従ってRREPのADD<sub>S</sub>, ADD<sub>D</sub>, Cert<sub>S</sub>, Sig<sub>S</sub>には、SとDの乱数系列のマスクがそれぞれ施されていることになる。

【0050】

中継端末T1, T2を経由して転送されたRREPを受信したSは以下の処理を行う。

【0051】

自分宛のRREPであるかどうかを検証する際に、受信端末Dが設定した疑似乱数系列を外す。これまで、対称鍵暗号の利用モードについては特に言及しなかったが、疑似乱数系列を出力するには、CTRモードでの利用が一般的である。

20

【0052】

図9にはCTRモードの概要を示している。Initialization Vector（以下IVと言う）は、送受信者間で秘密裏に共有できることが望ましい。カウンタ（以下ctと言う）は、送受信者間で同期する必要がある、同期外れの影響を減らすためには生値をパケットに付加して伝送することが望ましい。

【0053】

図10は、図8において対称鍵暗号の利用モードにCTRモードを想定した例である。図5と異なる処理を中心に以下に説明する。

30

【0054】

IVはSession Keyと接続して（以下“||”の記号で表示する）送信することとし、Seed=Session Key || IVとする。ctは、送信端末Sと受信端末Dで独立に選べるようにし（各々ct<sub>S</sub>, ct<sub>D</sub>とする）、パケットの先頭にこのフィールドを付加する。なおctがインクリメンタルに連続するとパケットの順序が第三者に漏れるため、送信者はランダムな値を割り当てることとする。またctはNonceの意味合いも含むため、今までED [Session Key] をNonceとして捉えていたが、以下ではctがNonceの役割を果たすものとする。

【実施例3】

【0055】

図11及び12を参照しながら、本発明の実施例3について説明する。図11は、図10と同様な図であるが、第三者に露呈される中継端末（ノード）に関する情報を網掛けで示している。中継情報の必要性について改めて考えると、送信端末Sと受信端末DはSource Routingを行うため全てのの中継端末の情報を知る必要があるが、中継端末自体は以下の判断ができれば十分である。

40

【0056】

1. RREQに対しては、自分宛であるかの確認、直前の中継端末からの情報の正当性。

【0057】

2. RREPに対しては、転送アドレスリストに自分が含まれるかどうか。

【0058】

従って不要な情報の露呈は攻撃の材料となる危険性があるため、中継端末の情報に関

50

しても可能な限り、送信端末Sと受信端末Dにしか分からないように隠蔽するのが望ましい。そこで、以下ではプライバシーの向上のために、図11の網掛けフィールドをSとDにしか分からないように隠蔽する例について説明する。

【0059】

図12は、図11の網掛けフィールドを隠蔽するために、RREQでは一時公開鍵を適用し、RREPでは対称鍵暗号の対象を拡大した例を示す。図8、図10と異なる処理を中心に以下に説明する。

【0060】

送信端末Sの乱数発生部430が、RREQの送信に当たり、一時公開鍵(K+)と一時秘密鍵(K-)のペアをランダムに決定する。一時公開鍵K+と一時秘密鍵K-とをRREQに追加して送信するが、一時秘密鍵K-のみ疑似乱数系列の排他的論理和の対象とする。

【0061】

RREQを受信した中継端末T2が、自分より以前の中継端末の情報(この場合ADD<sub>T1</sub>, Cert<sub>T1</sub>, Sig<sub>T1</sub>)をK+を用いて累積暗号化する。累積暗号化することによって、悪意のある中継端末が自分より以前の中継端末情報を逆順序で省略していった場合でも、受信端末Dで検出不可能となることを避けることができる。

【0062】

RREQを受信した受信端末Dは、以下の処理を行う。

【0063】

中継経路毎のSigを検証する。Sig<sub>T2</sub>を検証した後、ADD<sub>T2</sub>, Cert<sub>T2</sub>, Sig<sub>T2</sub>を除去する。中継端末の情報全体を一時秘密鍵K-を用いて復号する。Sig<sub>T1</sub>を検証する。ADD<sub>T1</sub>, Cert<sub>T1</sub>, Sig<sub>T1</sub>を除去する。Sig<sub>S</sub>を検証する。

【0064】

一般的には、次の一連の処理の中継端末情報全体の長さから推測される中継回数だけ繰り返すことになる。すなわち、一時秘密鍵K-で復号、最外側のSigの検証及び最外側の付加情報の除去の一連の処理である。

【0065】

受信端末Dが返信する際に、RREQからコピーした全ての情報に対して、受信端末Dで新たに作成した疑似乱数系列(受信時の乱数系列とは異なる)との排他的論理和を取って再暗号化し、RREPを作成する。マスクバタンの対象領域が拡大され、K-, K+, E<sub>D</sub>[Seed], ADD<sub>T1</sub>, Cert<sub>T1</sub>, Sig<sub>T1</sub>, ADD<sub>T2</sub>, Cert<sub>T2</sub>, Sig<sub>T2</sub>にもマスクボタンが掛かることになる。

【0066】

RREQからコピーした全ての情報にマスクボタンが掛けられているので、ADD<sub>T1</sub>とADD<sub>T2</sub>は隠蔽されており、中継端末において識別不可能となる。そこで、ADD<sub>T1</sub>とADD<sub>T2</sub>の生値を新設された中継アドレスリストフィールドに格納する。

【0067】

RREP信号を受信した送信端末Sは、以下の処理を行う。

【0068】

受信した被暗号化共通鍵E<sub>D</sub>[Seed]を復号化して、検証する。中継アドレスリストに自分のアドレスADD<sub>S</sub>を発見できないため、乱数系列を外す。ADD<sub>S</sub>, ADD<sub>D</sub>, Seed, Cert<sub>S</sub>, Sig<sub>S</sub>の組み合わせから、自分が以前に送信したRREQに対する応答であることを認識する。Sig<sub>D</sub>を検証する。中継経路毎のSigを検証する。すなわち、RREPをRREQに置きかえてSig<sub>D</sub>を除去する。Sig<sub>T2</sub>を検証した後、ADD<sub>T2</sub>, Cert<sub>T2</sub>, Sig<sub>T2</sub>を除去する。Sig<sub>T1</sub>を検証した後、ADD<sub>T1</sub>, Cert<sub>T1</sub>, Sig<sub>T1</sub>を除去する。中継経路情報(S→T1→T2→D)を確定する。

【実施例4】

【0069】

図13及び図14を参照しながら、本発明の実施例4について説明する。図13は、図12と同様な図であるが、第三者に露呈される中継端末(ノード)に関する情報を網掛けで示している。中継端末のアドレスに関しても可能な限り、送信端末Sと受信端末Dと中継

10

20

30

40

50



端末自身にしか分からないように隠蔽することが望ましい。そこで、プライバシーの向上のために、図13の網掛けフィールドを送信端末Sと受信端末Dと中継端末自身にしか分からないように隠蔽する実施例を説明する。

#### 【0070】

簡単な対処としては、 $ADD_{T1}$ 、 $ADD_{T2}$ を一時アドレスにする方法があるが、この方法だけでは複数のパケットを通じてしばらく同じ中継アドレスが適用されてしまうため、パケットの関連性が露呈する危険性が存在する。従って、パケット毎に異なる一時アドレスが適用される方が、よりプライバシーの漏洩に強い仕組みができる。この問題に対処するために、一時公開鍵とハッシュ関数の活用を考える。

#### 【0071】

図14は図13の網掛けフィールドを隠蔽するために、RREQでは乱数を一時公開鍵で暗号化し、RREPでは乱数にハッシュ関数を適用した例である。図9とは異なる処理を中心に以下に説明する。なお、 $rand_x$ とは端末Xで決定した乱数、 $h(y)$ とはyのハッシュ値を意味している。ハッシュ関数とは、ドキュメントや数字などの文字列の羅列から一定長のデータに要約するための関数・手順のことをいう。関数を通して出力される値は、「ハッシュ値」と呼ばれる。「SHA-1」と「MD5」というハッシュ関数が代表的で、いずれも1方向関数であるため、生成データから原文を推定することは不可能である。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないかを調べることができる。

#### 【0072】

RREQを受信した中継端末T1は、自己のアドレス $ADD_{T1}$ の代わりに $E_x$ 、 $[rand_{T1}]$ を設定する。

#### 【0073】

T2もT1と同様の処理を行う。

#### 【0074】

RREQを受信したDは、 $rand_{T1}$ 、 $rand_{T2}$ を取得し、 $ADD_{T1}$ 、 $ADD_{T2}$ の生値の代わりに、 $h(rand_{T1} || ct_D)$ 、 $h(rand_{T2} || ct_D)$ を適用する。

#### 【0075】

RREPを受信したT2は、自分のアドレスを $h(rand_{T2} || ct_D)$ として認識する。

#### 【0076】

T1もT2と同様の処理を行う。

#### 【0077】

RREPを受信した送信端末Sは以下の処理を行う。

#### 【0078】

中継アドレスリストで自分のアドレスを発見する際、 $h(rand_S || ct_D)$ を検査する。 $r_{and_{T1}}$ 、 $rand_{T2}$ を取得する。

#### 【実施例5】

#### 【0079】

図14乃至図16を参照しながら、本発明の実施例5について説明する。

#### 【0080】

図14を参照すると、RREQのパケット長やRREPの中継アドレスリストから、送信端末Sと受信端末Dに関する情報が以下のように漏れる危険性が高いことが分かる。

#### 【0081】

・RREQ: パケット長から、中継端末T1が受信端末Sの隣にいることが分かる。

#### 【0082】

・RREP: 中継端末T1と中継端末T2が結託（共謀）すれば、中継アドレスリストから、受信端末Dは中継端末T2の隣（SはT1の隣）であることが分かる。そこで、ダミー情報（乱数）を活用して送信端末S及び受信端末Dに中継端末であるかのように振舞わせることにより、送信端末Sと受信端末Dの情報を可能な限り隠蔽する例を説明する。

#### 【0083】

10

20

30

40

50

図15は、送信端末SからのRREQ信号及び受信端末DからのRREP信号の各々に、ダミー情報を付与して、両端末があたかも中継端末であるかのように振る舞わせたものである。前述の例とは異なる処理を中心に以下に説明する。送信端末Sは、RREQ信号中にダミーの中継端末情報(図15では1中継分を意味するDummy1, Dummy2)を付与する。ダミー情報が存在するために、送信端末Sの情報が露呈していても、第三者から見て、発信端末と中継端末との区別がつかない。

【0084】

RREQ信号を受信した中継端末T1は、Sig<sub>S</sub>の検証を行う。直前上記の例ではSig<sub>S</sub>の検証ができなかったで、特定の長さのRREQはSからのRREQであると想定してSig<sub>S</sub>の検証は行わなかった。本実施例では、Sが中継端末のふりをするため証明書Cert<sub>S</sub>を明かせるようになり、認証が可能になった。

【0085】

RREQを受信したDは以下の処理を行う。

【0086】

一時秘密鍵K<sub>r</sub>を用いて復号化し、中継経路毎のSigを再外側から順番に検証していき、Cert<sub>S</sub>が出現するまで検証処理を繰り返す。直前上記の例では中継ノード情報全体の長さから推測される中継回数だけ処理を繰り返していたが、本実施例では、Sが中継端末のふりをするため、その方法は適用できない。

【0087】

受信端末Dにおいて、RREP信号の中継アドレスリストに、ダミーアドレス(図15では2つ分のDummyADD1, DummyADD2)を付加し、疑似乱数系列との排他的論理和を取る。

【0088】

RREP信号を受信した送信端末Sは、中継経路毎のSigの検証を送信端末Dと同様に行う。

【0089】

ここで、図15を良く見ると、RREP信号のパケット長さから、中継段数に関する情報が漏れる危険性があることが分かる。そもそもRREP信号の内容は送信端末S及び受信端末Dだけが認識できれば十分であり、第三者が識別をする必要はない。そこで、RREP信号の素性を可能な限り隠蔽する例について以下に説明する。

【0090】

図16は、RREPの素性を可能な限り隠蔽した例である。前述の例と異なる処理を中心に以下に説明する。

【0091】

受信端末Dは、RREP信号の作成にあたり、以下の処理を行う。

【0092】

RREPの代わりに、送信端末SのみがRREPかDataかを判別できる第2の識別フィールド(RREP/Data)を追加する。ダミー情報(乱数)のパディングを追加する(図16におけるDummy Padding)。Lengthフィールドを追加して、Dummy Paddingを除く長さを設定する。第2の識別フィールド、Dummy Padding、Lengthの3つには、受信端末Dが設定したマスクボタンをかける。

【0093】

RREP/Dataを受信した送信端末Sは、受信端末Dが設定したマスクボタンを外した後に、以下の処理を行う。

【0094】

1. 第2の識別フィールドからRREPであることを認識する。

【0095】

2. Lengthフィールドを考慮して、Dummy Paddingを除去する。

【実施例6】

【0096】

図17に本発明の実施例6を示す。図17に示す実施例6は、上記実施例を全て含んだ態様の例である。従って、説明を省略する。

10

20

30

40

50

## 【実施例 7】

## 【0097】

次に、仮に T2 が悪意のある中継端末であるとする、中継端末 T2 が中継端末 T1 の情報を故意に破棄してしまうことがあり得る。そこで、そのような悪事に対処するための例について以下に説明する。

## 【0098】

図 17 を参照して説明する。中継端末 T1 の情報とその直前の端末 Dummy2 の情報とに不可分な関連を持たせることで、中継端末 T1 の情報が破棄されたことを見破る仕組みを考える。

## 【0099】

図 18 に示すように、中継端末 T1 において、その直前の端末である Dummy2 の情報に対して、中継端末 T1 の情報に基づく  $K_{T1} = h(\text{rand}_{T1}, \text{Cert}_{T1})$  を鍵とするブロック暗号による暗号化を施す。 $\text{rand}_{T1}$  とは端末 T1 で決定した乱数、 $\text{Cert}_{T1}$  は、証明書発行部が発行する端末 T1 の証明書であり、 $h(y)$  とは  $y$  のハッシュ値を意味している。

## 【0100】

中継端末 T2 においても、その直前の端末である T1 の情報に対して、中継端末 T2 の情報に基づく  $K_{T2} = h(\text{rand}_{T2}, \text{Cert}_{T2})$  を鍵とするブロック暗号による暗号化を施す。従って、この暗号化を復元するには、受信端末 D は、正しい中継端末情報を知る必要がある。

## 【0101】

Dummy を用いた場合を例にとり本実施例を説明したが、本実施例に係る発明は実存する中継端末に関しても応用可能であり、それ以外の多種多様な構成に対しても応用可能である。直前の端末情報に限らず上流の任意の端末情報を暗号化しても良い。

## 【0102】

上記のような構成を備えることによって、もし悪意のある中継端末が上流の中継端末の情報を故意に破棄したとしても、受信端末 D において、破棄された中継端末直前の端末の情報が正しく復号されないことになる。こうして受信端末 D は、この偽造経路を見破ることができる。

## 【0103】

このように、本実施例によれば、中継端末による処理負荷をそれほど大きくすることなく、悪意の中継端末による中継端末情報の偽造を防止することができ、偽造不可能なように経路情報を隠蔽可能であり、第三者に対する送受信者のプライバシーが向上される。

## 【産業上の利用可能性】

## 【0104】

本発明に従った、通信端末及びアドホックネットワーク経路制御方法は、秘匿が要求される無線又は有線通信分野において利用することができる。

## 【図面の簡単な説明】

## 【0105】

【図 1】従来のアドホックネットワークの概略を示す概念図である。

【図 2】従来のアドホックネットワーク構築可能な移動端末の概略ブロック図である。

【図 3】従来のアドホックネットワーク構築のための経路制御信号のデータを示すチャートである。

【図 4】本発明の実施例に従った移動端末のブロック図である。

【図 5】実施例 1 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートである。

【図 6】実施例 2 を説明するための経路制御信号のデータを示すチャートであり、第三者への送受信端末の露呈が示されている。

【図 7】実施例 2 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ADDS に一時アドレスを使用している。

【図 8】実施例 2 に従った、アドホックネットワーク構築のための経路制御信号のデータ

を示すチャートであり、ハイブリッド暗号を使用している。

【図 9】実施例 2 に従った、CTR モードの概要を示す概念図である。

【図 10】実施例 2 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、CTR モードを使用している。

【図 11】実施例 3 を説明するための経路制御信号のデータを示すチャートであり、第三者への中継情報の露呈が示されている。

【図 12】実施例 3 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、一時公開鍵を使用している。

【図 13】実施例 4 を説明するための経路制御信号のデータを示すチャートであり、第三者への中継端末アドレスの露呈が示されている。

【図 14】実施例 4 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハッシュ関数の利用を示している。

【図 15】実施例 5 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ダミー情報が付加されている。

【図 16】実施例 5 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、RREP の素性を可能な限り隠蔽した例である。

【図 17】各実施例の全て含んだ、アドホックネットワーク構築のための経路制御信号のデータを示すチャートである。

【図 18】実施例 7 に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、中継端末の破壊を防止する例である。

【符号の説明】

【0106】

- 400 移動端末
- 422 リクエスト／リプライ発生部
- 424 制御部
- 426 送受信部
- 427 アドレス記憶部
- 428 アドレス比較部
- 430 乱数発生部
- 440 証明書発行部
- 450 デジタル署名作成部
- 460 秘密鍵処理部
- 470 演算部
- 480 検証部

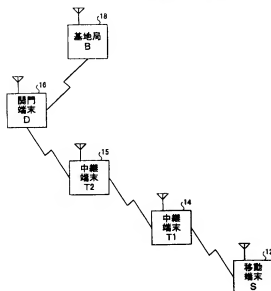
10

20

30

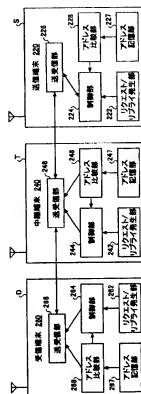
【図 1】

従来のアドホックネットワークの概略を示す概念図



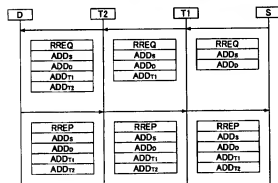
【図 2】

従来のアドホックネットワーク構築可能な移動端末の概略ブロック図



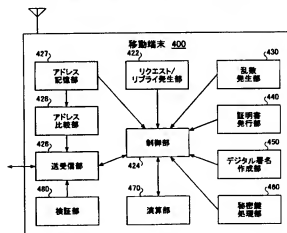
【図 3】

従来のアドホックネットワーク構築のための経路制御信号のデータを示すチャート



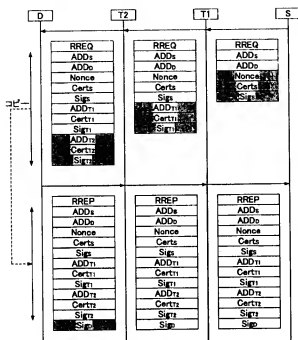
【図 4】

本発明の実施例に依った移動端末のブロック図



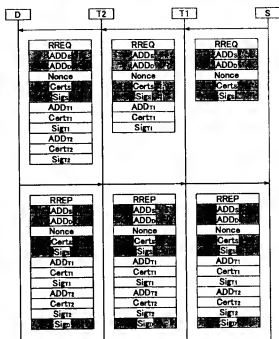
【図 5】

実施例1に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャート



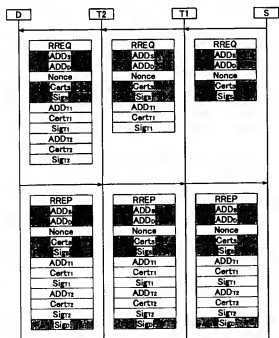
【図 6】

実施例2を説明するための経路制御信号のデータを示すチャートであり、第三者への送受信端末の露呈が示されている図



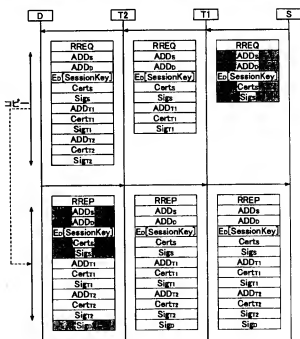
【図 7】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ADDSに一時アドレスを使用している図



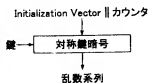
【図 8】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハッシュ値の露呈が示されている図



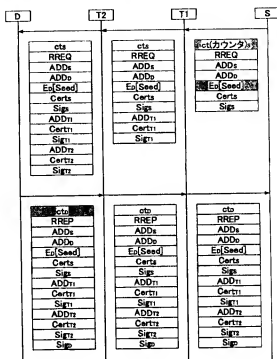
【図9】

実施例2に従った、CTRモードの概要を示す概念図



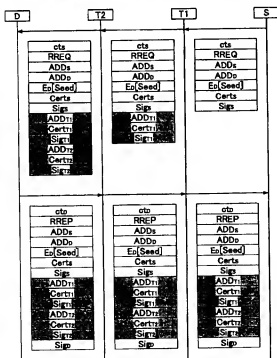
【図10】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、CTRモードを使用している図



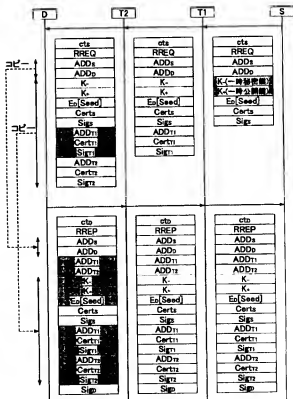
【図11】

実施例3を説明するための経路制御信号のデータを示すチャートであり、第三者への中間情報の漏洩が示されている図



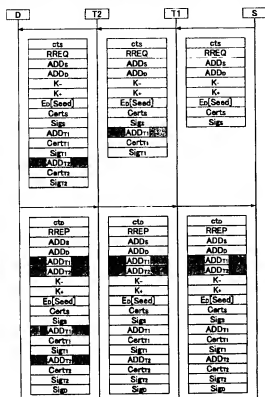
【図12】

実施例3に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、一時的公開鍵を使用している図



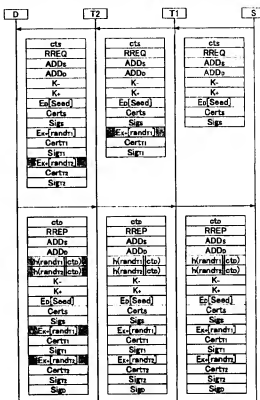
【図 13】

実施例4を説明するための経路制御信号のデータを示すチャートであり、第三者への中間端末アドレスの露出が示されている図



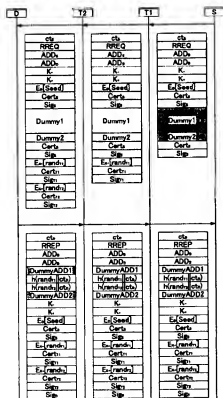
【図 14】

実施例4に基づた、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハッシュ関数の利用を示している図



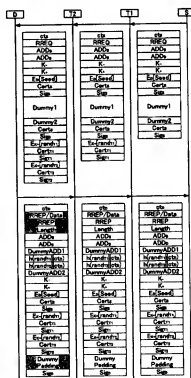
【図 15】

実施例5に基づた、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ダミー情報が付加されている図



【図 16】

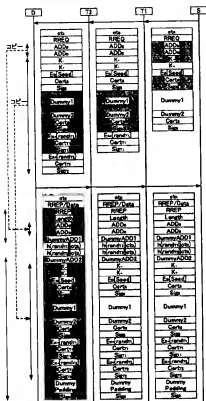
実施例5に基づた、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、RREPの素性を可能な限り隠蔽した例





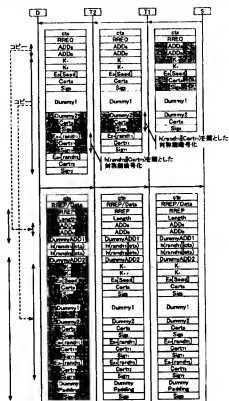
【 17 】

各実施例の全てを含んだ、アドホックネットワーク構築のための経路制御信号のデータを示すチャート



【 18 】

実施例7に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、中継端末の破壊を防止する例



---

フロントページの続き

Fターム(参考) SK033 AA09 CB01 DA05 DA19 DB18 EC03